Federal Motor Carrier Safety Administration (FMCSA)

Information Technology Systems

Rules of Behavior

As a user of the Federal Motor Carrier Safety Administration Information Technology (FMCSA IT) Systems, I understand that I am personally responsible for the use and any misuse of my system account and password. I also understand that by accessing a U.S. government information system that I must comply with the following requirements:

1. FMCSA IT systems are intended for official government use only. Limited personal use may be authorized at the discretion of the supervisor.
2. FMCSA IT systems may not be used for commercial purposes, for financial gain, or in support of "for profit" non-government activities.
3. The government reserves the right to monitor the activity of any machine connected to its infrastructure.
4. FMCSA IT systems are the property of the Federal government. FMCSA owns the data stored on these systems, including all email messages and information, even those deemed personal.
5. Sensitive information may not be transmitted at a level higher than what the system is approved for.
6. Information that was obtained via FMCSA IT systems may not be divulged outside of government channels without the express permission of the owner of that information.
7. Any activity that would discredit FMCSA, including seeking, transmitting, collecting, or storing defamatory, discriminatory, obscene, harassing, or intimidating messages or material is not permitted.
8. Any activity that violates Federal laws for information protection (e.g., hacking, spamming, etc) is not permitted.
9. FMCSA IT system accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism **must** never be shared or stored **in printed form** any place accessible. If stored **digitally**, a password must not be stored in a clear-text or readable format.
10. Each FMCSA IT system has password format requirements and a password expiration policy. Although there are variations between systems, passwords which are at least 8 alphanumeric characters in length, and contain at least two letters and three numbers or special characters (@, $, #, etc.) will normally meet the requirement. Typically, passwords must be changed every 90 days (30 days for Administrator accounts).
11. Virus prevention tools must be installed and kept current on any and all machines from which FMCSA IT systems are accessed.

12. Any security problems or password compromises must be reported immediately to the FMCSA Information Systems Security Officer (ISSO) at FMCSA Headquarters (MC-RIS) and local FMCSA IT security personnel.
13. Telecommuters are required to review and adhere to the Remote Access Policy.
14. Users of FMCSA IT systems are prohibited from modifying their systems by: installing unapproved hardware, installing additional operating systems, installing unapproved software applications, or altering approved configuration settings.
15. Users of FMCSA IT systems may not communicate FMCSA information to external news groups, bulletin boards, or other public forums without permission.
16. Users of FMCSA IT systems may not access services with the potential to degrade network performance. This includes: use of a program or Internet site that provides continuous data streams, e.g., continuous stock quotes, or headline news updates, etc.
17. Users in possession of an FMCSA-issued Blackberry must sign an additional Rules of Behavior document specific to the use of their Blackberry.
18. Users may not connect unauthorized devices (non FMCSA issued) to the network without approval as documented in the Network Access policy.
19. Laptops must be stored in a secure location to prevent theft. FMCSA-issued laptops should not be left in plain sight in vehicles. If you must leave your laptop in an unattended vehicle, secure it in a locked trunk, or otherwise ensure that it is completely out of sight.
20. Every FMCSA-issued laptop has standard security controls enabled at all times. Standard security controls include host-based firewall and anti-virus software, and an anti-spyware scanner. Laptop users must never tamper or attempt to circumvent the purpose or implementation of these controls.
21. When using FMCSA-issued laptops, password authentication must be enabled.
22. Users must encrypt all personally identifiable information (PII) whenever it resides on laptops, mobile devices, and storage media devices that carry PII data.

I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to 10 years in jail for the first offense for anyone who:

a) Knowingly accesses an information system without authorization, or exceeds authorized access and obtains information that requires protection against unauthorized disclosure.

b) Intentionally, without authorization, accesses a Government information system and impacts the Government’s operation, including availability of that system.

c) Intentionally accesses a Government information system without authorization, and alters, damages or destroys information therein.

d) Prevents authorized use of the system or accesses a Government information system without authorization, or exceeds authorized access, and obtains anything of value.

My signature below indicates that I have read, have understood, and will comply with the above stated requirements as a condition of maintaining active accounts with access to FMCSA IT systems. I also understand that failure to comply with these requirements may result in disciplinary action.

Name: ______________________________ Telephone: ______________________

(First MI Last)

Organization: ________________________ State: ___________________

Office Symbol or Org Code: __________________

Email Address: ____

Signature: ___________________________________ Date: ____________

Updated 19 September 2006